REMARKS

In the Office Action mailed March 09, 2006, the examiner rejected claims 66-102 under 35 U.S.C. 103(a) as being unpatentable over Wagener (U.S. Pat. No. 5,793,028), Bramhill (WO 98/44402) and Wray (GB 2355322A). Applicant filed a response detailing why applicant believes that the present invention, as defined by the claims, is distinguishable over Wagener, Bramhill and Wray. The examiner mailed an Advisory Action on May 26, 2006, stating only that applicant's arguments (running to 11 pages) were "not persuasive." Applicant, however, respectfully disagrees and requests that the examiner reconsider.

The present invention, as defined by amended claim 66, relates to a network system. The network system includes a first computer arrangement and a second computer arrangement connected by a computer network. The second computer arrangement stores data and executable fingerprint software. The executable fingerprint software includes a plurality of instructions readable and performable by the first computer arrangement. The first computer arrangement is programmed to transmit a request for data to the second computer arrangement, receive the executable fingerprint software from the second computer arrangement, execute the executable fingerprint software, and receive the requested data from the second computer arrangement. When the first computer arrangement executes the executable fingerprint software by reading and performing the plurality of instructions, the first computer arrangement creates fingerprint data that is substantially unique to the first computer arrangement and transmits the fingerprint data to the second computer arrangement. The second computer arrangement is programmed to receive a request for data from the first computer arrangement, transmit the executable fingerprint software to the first computer arrangement in response to receiving the request, receive fingerprint data from the first computer arrangement, and transmit the requested data to the first computer arrangement in response to receiving the fingerprint data.

Applicant submits that amended claim 66 is no different in scope than the previously presented version of claim 66. The only purpose of the amendment is to state certain limitations of the claim explicitly. That is, in the context of claim 66 applicant submits the term "software" would be understood by one of ordinary skill in the art to be instructions readable and performable by a computer (as opposed to data, for example, which would merely be readable). Similarly, the term "execute" when used as a verb acting on "software" would be understood by one of ordinary skill in the art to mean the reading and performing of the instructions by a computer. In a telephone conversation with applicant's representative on or about May 31, 2006, the examiner indicated that the term execute was being interpreted as being equivalent to the term "use." While applicant is aware the examiner must use the "broadest reasonable" definition of a given term in performing the examination, applicant respectfully submits that the examiner's interpretation is so broad as to not be "reasonable." When claim 66 recites that the second computer arrangement "execute[s] the fingerprint software," applicant submits that a person of ordinary skill in the art would interpret that limitation as meaning the second computer arrangement reads and performs the instructions which make up the fingerprint software and not as meaning the second computer arrangement merely 'uses' the fingerprint software in some general, undefined manner. In short, if the fingerprint software was not "executable" and execution of the fingerprint software did not have the meaning given above, the fingerprint software would not in fact be "software" as that term is commonly understood. This clarification of the meaning of the terms "software" and "execute" is the only change to claim 66 resulting from the amendment.

The explanation above applies equally to amended claims 76, 81, 90, 98, and 102. Claims 72, 86 and 96 have been amended to correct a simple spelling error. Applicant therefore respectfully requests that the examiner enter the above amendments. Because

the scope of the claims is unchanged by the submitted amendments, as described above, applicant also submits that no further consideration or search is required for the examination of the claims.

The examiner alleges that Wagener describes a first computer that: transmits a request for data to a second computer; executes fingerprint software to create fingerprint data; transmits fingerprint data to the second computer; and receives the requested data. Additionally, the examiner alleges that Wagener describes a second computer that: stores a copy of the fingerprint software that is executed by the first computer; receives from the first computer a request for data; transmits the fingerprint data to the first computer in response to receiving the request; receives fingerprint data from the first computer; and transmits the requested data to the first computer in response to receiving the fingerprint data.

Wagener is described in detail in applicant's previous response. In sum, Wagener describes a security system for performing electronic transactions. When an individual (transactionor) wishes to perform a transaction with another individual (transactionee), the security system first verifies, via a third individual (verifier), that the identities of the individuals are genuine. Each transactionor and transactionee is provided with a unique public identification code and a unique private identification code (col. 3, lines 37-58 of Wagener). The public identification code is used to identify each individual and is used by the security system for addressing purposes. For example, a transactionor uses the public identification code to specify that a transaction is to be carried out with the transactionee having that particular public identification code. Whilst the public identification code is publicly available, the private identification code is known only to the transactionor or transactionee and to the verifier. Importantly, the private identification code of a transactionor is not known by the transactionee, and vice versa. The verifier

is also provided with a public identification code, so that the verifier can be identified and addressed by both the transactionor and the transactionee.

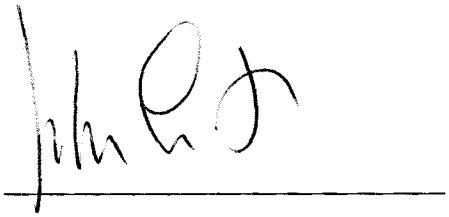
The examiner acknowledges that Wagner does not teach a "first computer arrangement" that is programmed to "receive fingerprint software from the second computer arrangement" in the sense of claim 66. However, the examiner alleges that Wray teaches a system whereby fingerprint software is stored on a second computer and is transmitted to the first computer in response to a request for data. In particular, the examiner alleges that the receiving step 200 of Figure 8 and the setup step 400 of Figure 12 of Wray, as well as their respective explanations in the specification, teach such an arrangement.

Wray is described in detail in applicant's previous response. In sum, Wray describes a system for positively identifying a client terminal that attempts to communicate with a host machine (e.g. page 15, lines 9-11 of Wray). The client terminal and the host machine respectively have EPCI software and ASR software installed thereon. The EPCI software creates a client identifier key (CIK), which includes data that are unique to the hardware and software configuration of the client terminal (page 29, lines 9-13). When the client terminal attempts to communicate with the host machine, the ASR software requests that the CIK of the client terminal be returned. The EPCI software then creates a CIK for the client terminal and compares this against a previously-created CIK that is stored on the client terminal; this then prevents illegal copying of the EPCI software to a different client terminal. If the newly-generated CIK corresponds to the previously-created CIK, the EPCI software sends the newly-generated CIK to the host machine. The ASR software is then able to positively identify the client terminal from the CIK (page 29, lines 9-15 of Wray).

None of the communication between the client and host machines involves the exchange of software. Rather, software *already present* on both machines is executed.

Applicant therefore submits that, for the reasons provided in the previous response and elaborated on above, amended claim 66 of the present application is patentable over Wagener when considered in combination with Bramhill and Wray. It follows that dependent claims 66-75 are also patentable. Applicant further submits that the arguments previously submitted and elaborated on above are equally applicable to amended claims 76, 81, 90, 98 and 102 and therefore those claims are also patentable over Wagener when considered in combination with Bramhill and Wray. It follows that dependent claims 77-80, 82-89, 91-97, and 99-101 are also patentable.

Respectfully submitted,



John Smith-Hill

Reg. No. 27,730

SMITH-HILL & BEDELL, P.C.
16100 N.W. Cornell Road, Suite 220
Beaverton, Oregon 97006

Tel. (503) 574-3100
Fax (503) 574-3197
Docket: SWIN 2276